Configuring Authentication

This chapter explains how to configure the authentication portion of Cisco's authentication, authorization and accounting (AAA) services on the SN 5428-2 Storage Router and how to configure Enable, Login and iSCSI authentication, which use AAA services.

The following tasks are covered:

The AAA function is always enabled for the storage router; it cannot be disabled.

Authentication parameters can be configured using CLI commands, as described in this chapter, or via the web-based GUI. To access the web-based GUI, point your browser to the storage router's management interface IP address. After logging on, click the Help link to access online help for the GUI.

Prerequisite Tasks

Before performing AAA configuration tasks on the storage router, make sure you have configured system parameters as described in Chapter 2, "First-Time Configuration," or Chapter 3, "Configuring System Parameters." If the storage router is deployed for SCSI routing, you should also configure SCSI routing instances as described in Chapter 6, "Configuring SCSI Routing," before proceeding. See the iSCSI driver readme file for details on configuring IP hosts for iSCSI authentication.

Note AAA configuration settings are cluster-wide elements and are shared across a cluster. All AAA configuration and management functions are performed from a single storage router in a cluster. Issue the **show cluster** command to identify the storage router that is currently performing AAA configuration and management functions.

Using Authentication

AAA is Cisco's architectural framework for configuring a set of three independent security functions in a consistent, modular manner. Authentication provides a method of identifying users (including login and password dialog, challenge and response, and messaging support) prior to receiving access to the requested object, function, or network service.

The SN 5428-2 Storage Router implements the authentication function for three types of authentication:

- iSCSI authentication—provides a mechanism to authenticate all IP hosts that request access to storage via a SCSI routing instance. IP hosts can also verify the identity of a SCSI routing instance that responds to requests, resulting in two-way authentication.
- Enable authentication—provides a mechanism to authenticate users requesting access to the SN 5428-2 in Administrator mode via the CLI **enable** command or an FTP session.
- Login authentication—provides a mechanism to authenticate users requesting access to the SN 5428-2 in Monitor mode via the login process from a Telnet session, SSH session or the management console.

iSCSI Authentication

When enabled, iSCSI drivers provide user name and password information each time an iSCSI TCP connection is established. iSCSI authentication uses the iSCSI Challenge Handshake Authentication Protocol (CHAP) authentication method.

iSCSI authentication can be enabled for specific SCSI routing instances. Each SCSI routing instance enabled for authentication can be configured to use a specific list of authentication services, or it can be configured to use the default list of authentication services.

For IP hosts that support two-way authentication, the SCSI routing instance can also be configured to provide user name and password information during the iSCSI TCP connection process.

Note iSCSI authentication is available for SN 5428-2 storage routers deployed for SCSI routing or transparent SCSI routing only; it is not available for storage routers deployed for FCIP.

Enable Authentication

When configured, a user enters password information each time the CLI **enable** command is entered from the management console, or from a Telnet or SSH management session. If the storage router is configured to allow FTP access, Enable authentication also authenticates users attempting to login and establish an FTP session with the storage router.

Using RADIUS Security Servers

Because the **enable** command does not require you to enter a user name, RADIUS authentication services are passed the default user name, *$enab15$,* along with the entered password for authentication. If no authentication services are configured, the entered password is checked against the Administrator mode password configured for the storage router.

Using TACACS+ Security Servers

Because the **enable** command does not require you to enter a user name, TACACS+ authentication services are passed the user name used at login, along with the entered password, for authentication. If a user name was not needed for login, the storage router will prompt the user to enter a user name, along with the enable password, when the **enable** command is issued.

Login Authentication

When configured, you are prompted to enter a user name and password each time access to the storage router is attempted from the management console, or from a Telnet or SSH management session.

Authentication Services

Authentication is configured by defining the authentication services available to the storage router. iSCSI, Enable and Login authentication types use authentication services to administer security functions. If you are using remote security servers, AAA is the means through which you establish communications between the SN 5428-2 and the remote RADIUS or TACACS+ security server.

Table 9-1 lists the authentication services and indicates which authentication types can be performed by each service.

Table 9-1 Authentication Services

Authentication Service	Description	Authentication Types
RADIUS	A distributed client/server system that secures networks against unauthorized access. The SN 5428-2 sends authentication requests to a central RADIUS server that contains all user authentication and network service access information.	All
TACACS+	A security application that provides centralized validation of users. TACACS+ services are maintained in a database on a TACACS+ daemon running, typically, on a UNIX or Windows NT workstation.	All

Table 9-1 Authentication Services (continued)

Authentication Service	Description	Authentication Types
Local or Local-case	Uses a local username database on the storage router for authentication. Local-case indicates that the user name authentication is case-sensitive. Passwords authentication is always case-sensitive.	Login and iSCSI authentication only
Enable	Uses the Administrator mode password configured for the storage router.	Enable and Login authentication only
Monitor	Uses the Monitor mode password configured for the storage router.	Enable and Login authentication only

Configuration Tasks

To configure iSCSI, Enable or Login authentication and the associated authentication services on the storage router, perform the following steps:

Step 1 Configure the desired authentication services, such as RADIUS, TACACS+ and the local username database.

Step 2 (Optional) Create named groups of RADIUS and TACACS+ servers.

Step 3 Create authentication lists.

Step 4 (Optional) Test authentication using configured authentication services.

Step 5 (Optional) Configure the user name and password for SCSI routing instances that will participate in two-way authentication.

Step 6 Enable authentication for individual SCSI routing instances.

Step 7 Verify and save AAA and iSCSI authentication configuration.

Figure 9-1 illustrates AAA configuration elements used for iSCSI authentication and Figure 9-2 illustrates the example configuration of iSCSI authentication and the authentication services used in this chapter.

Figure 9-1 iSCSI Authentication Configuration Elements

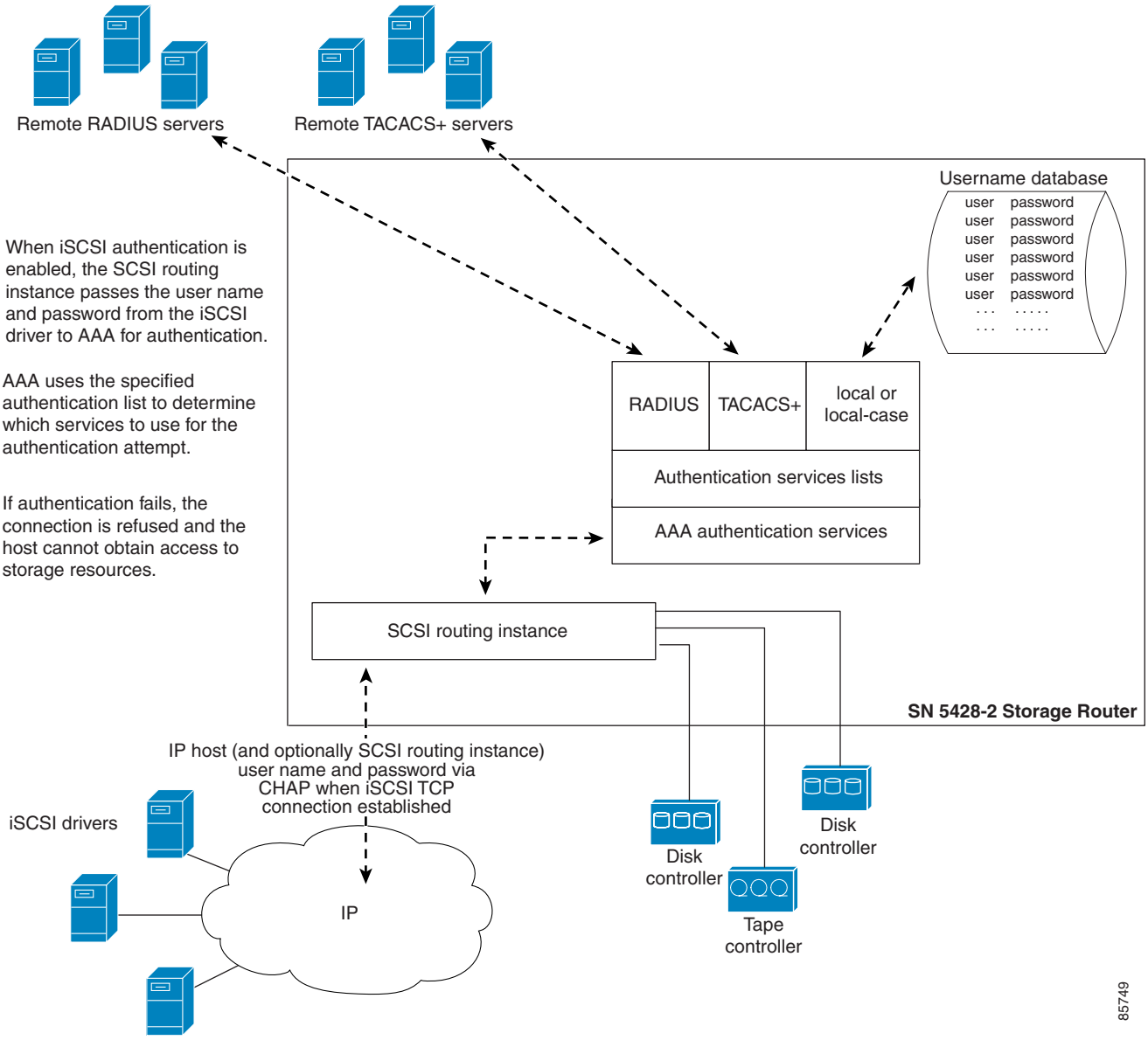


Figure 9-2 iSCSI Authentication Example Configuration

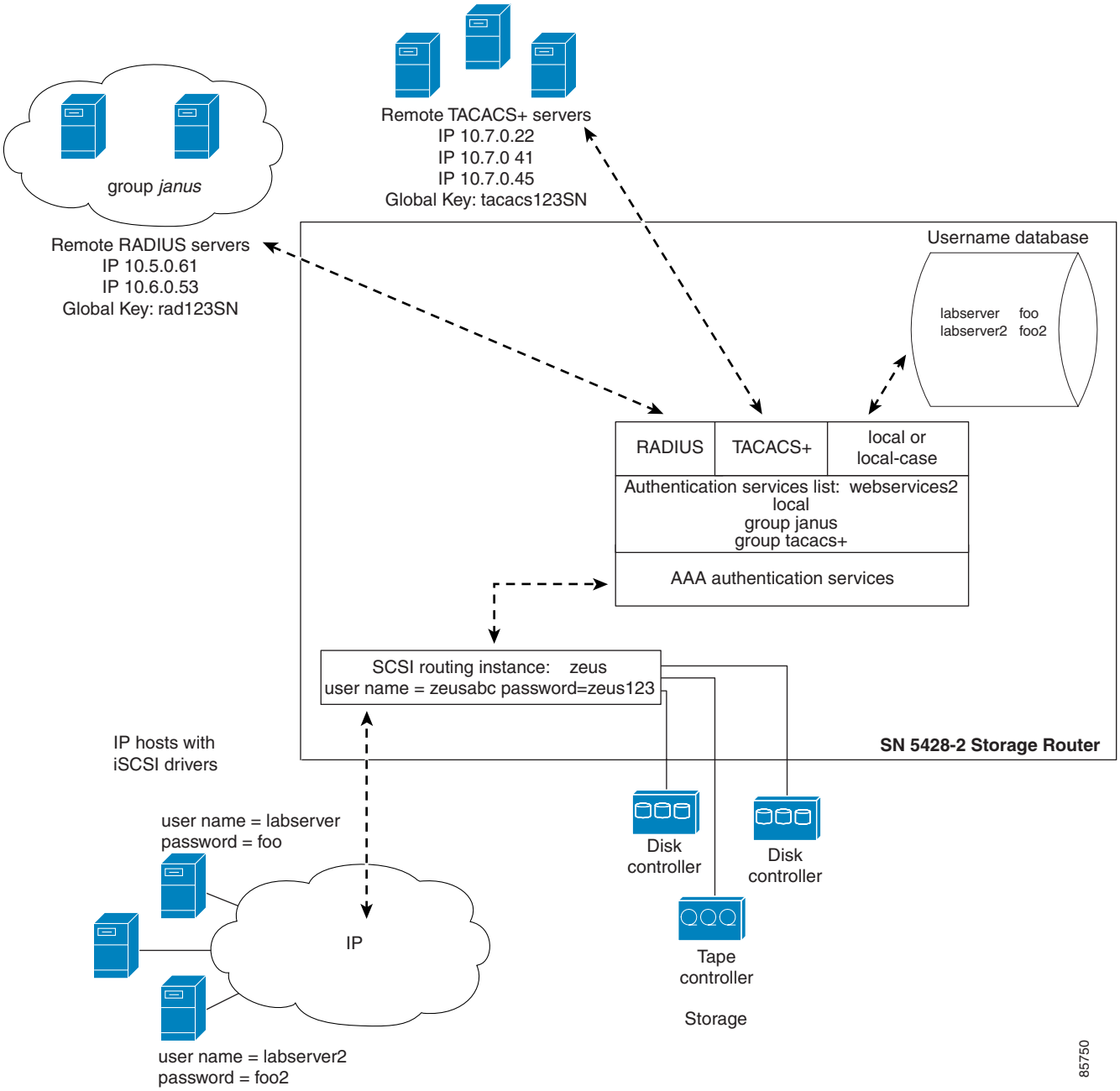


Figure 9-3 illustrates AAA configuration elements used for Enable authentication with RADIUS servers, Figure 9-4 illustrates AAA configuration elements used for Enable authentication with TACACS+ servers, and Figure 9-5 illustrates the example configuration of Enable authentication and the authentication services used in this chapter.

Figure 9-3 Enable Authentication Configuration Elements with RADIUS Servers

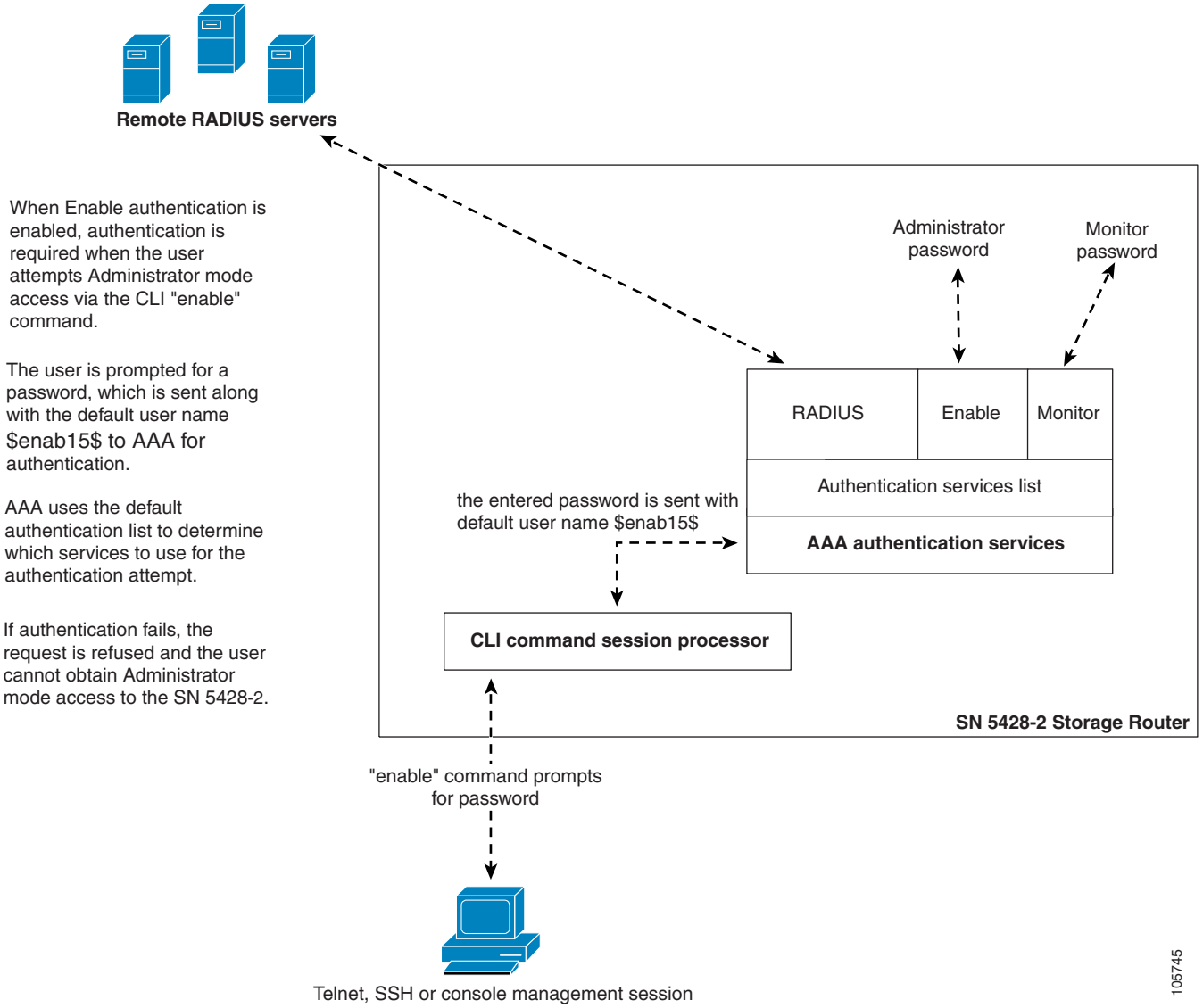


Figure 9-4 Enable Authentication Configuration Elements with TACACS+ Servers

When Enable authentication is enabled, authentication is required when the user attempts Administrator mode access via the CLI "enable" command.

The user is prompted for a password, which is sent along with the user name entered at login, to AAA for authentication.

If the user name was not needed for login, the storage router prompts the user to enter a user name along with the password, and both are sent to AAA for authentication.

AAA uses the default authentication list to determine which services to use for the authentication attempt.

If authentication fails, the request is refused and the user cannot obtain Administrator mode access to the storage router.

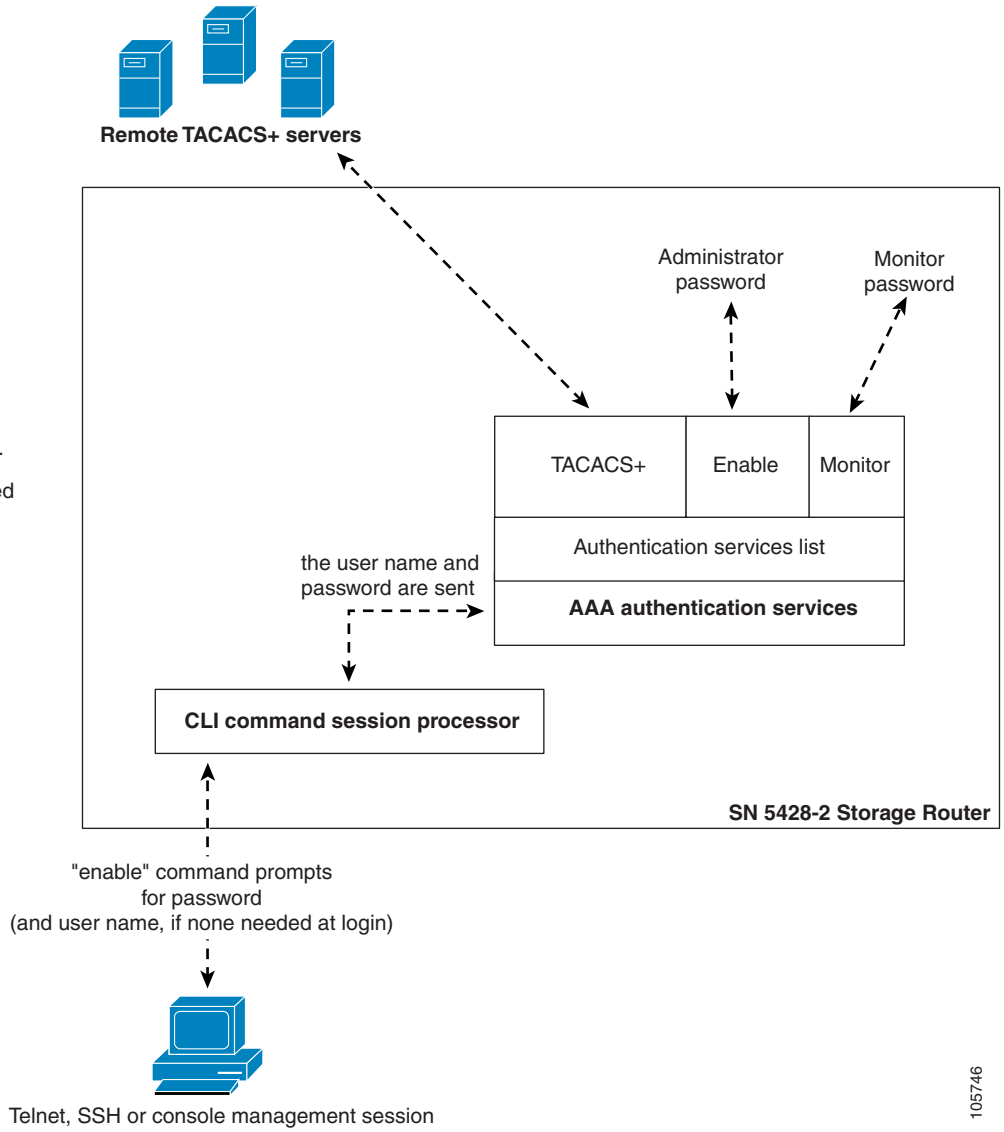


Figure 9-5 Enable Authentication Example Configuration

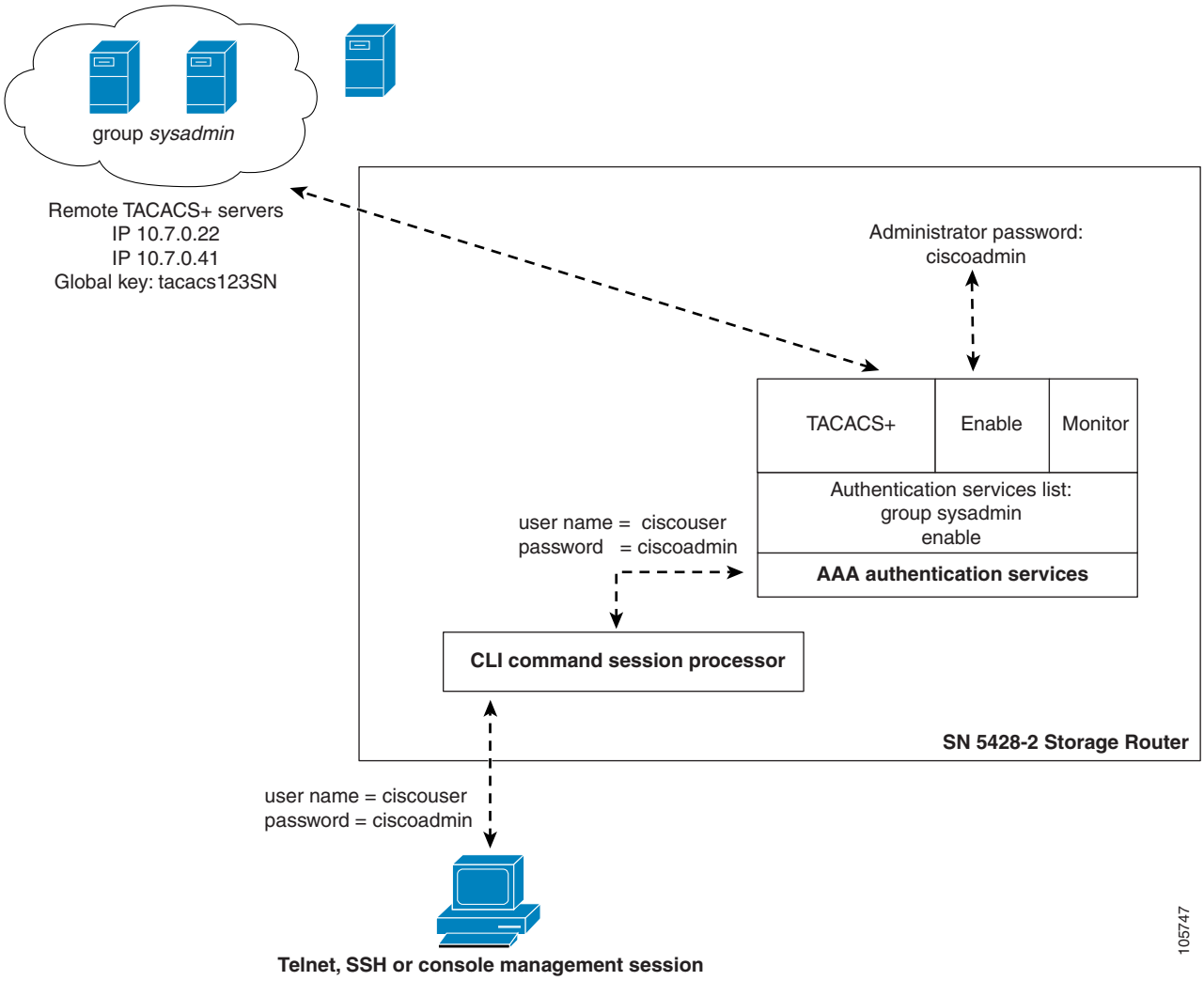


Figure 9-6 illustrates AAA configuration elements used for Login authentication and Figure 9-7 illustrates the example configuration of Login authentication and the authentication services used in this chapter.

Figure 9-6 Login Authentication Configuration Elements

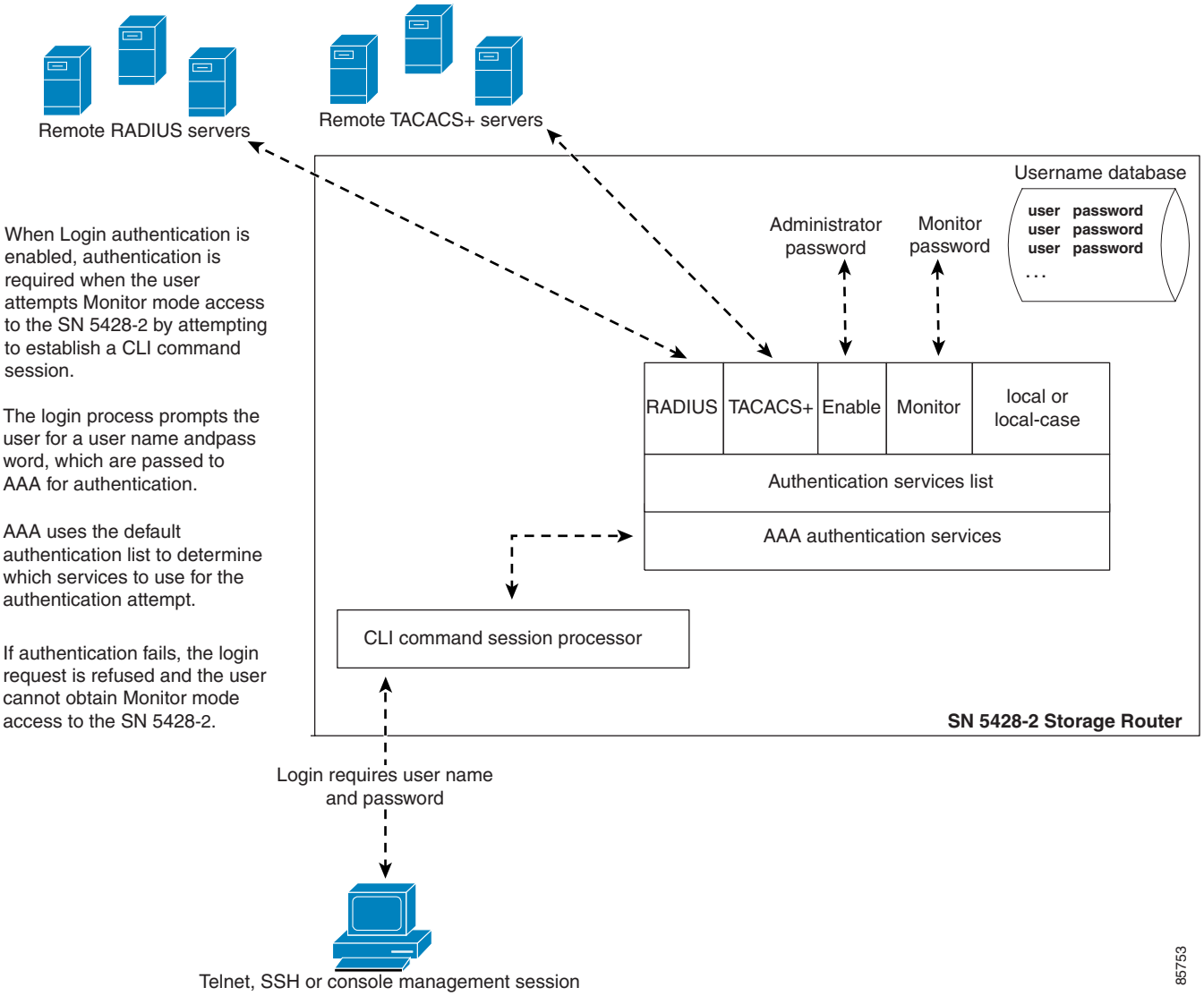
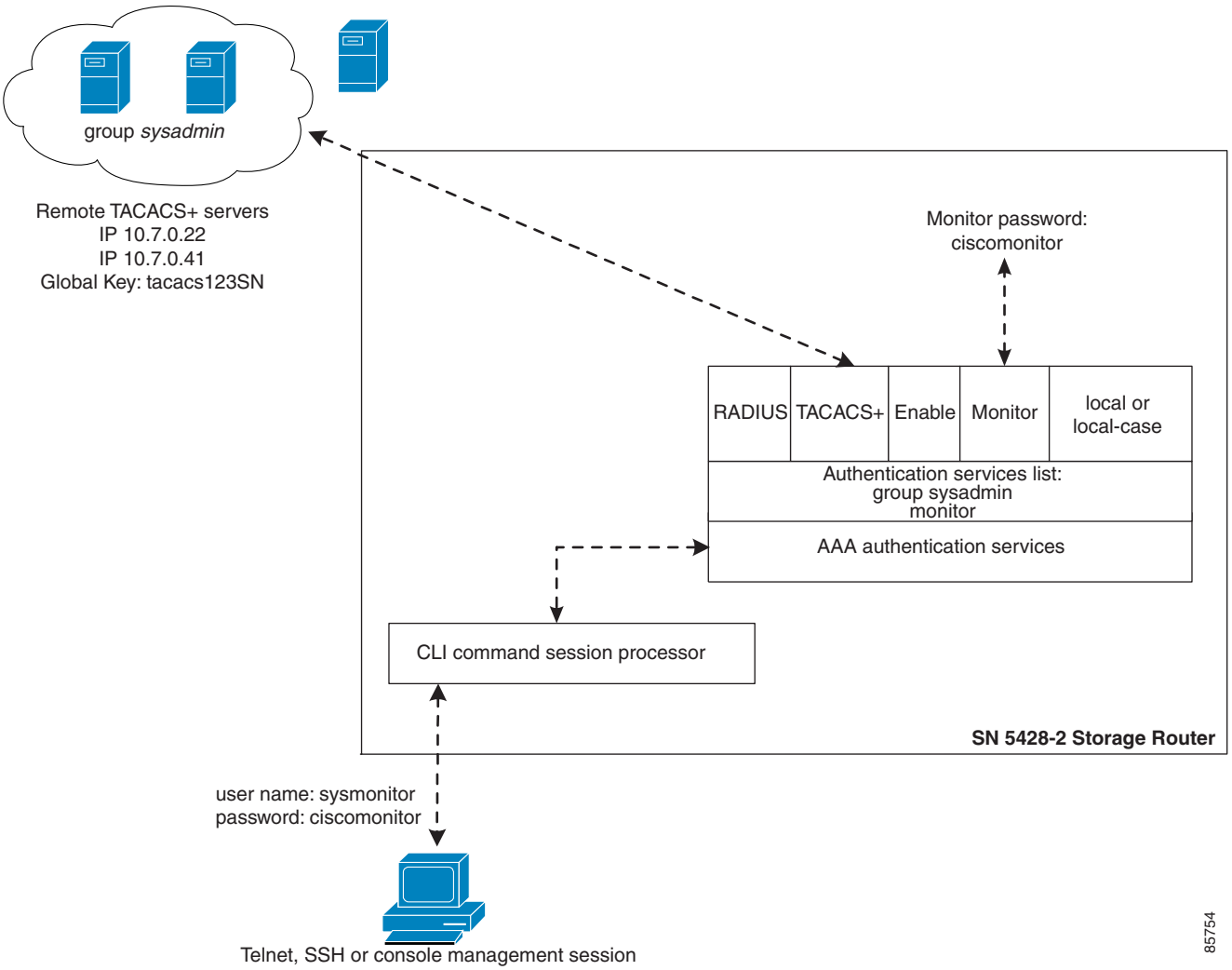


Figure 9-7 Login Authentication Example Configuration



Configuring Authentication Services

Configuring authentication services consists of setting the appropriate parameters for the various AAA service options that can be used by the storage router. The storage router can use any or all of the supported services:

- RADIUS
- TACACS+
- Local username database
- Enable
- Monitor

Use the procedures that follow to configure the storage router to use each of these services.

Note See the iSCSI driver readme file for details on configuring CHAP user names and passwords for iSCSI authentication.

RADIUS Servers

Use the commands in the following procedure to configure RADIUS authentication services.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**radius-server host** *10.6.0.53*	Specify the RADIUS server to be used for authentication. For example, specify the RADIUS server at *10.6.0.53* for use by the storage router. Because no port is specified, the authentication requests use the default UDP port 1645. Global timeout and retransmit values are also used. See the *Cisco SN 5400 Series Storage Router Command Reference* for more information about the **radius-server host** command.
Step 3	**radius-server host** *10.6.0.73* **radius-server host** *10.5.0.61*	Specify additional RADIUS servers. For example, specify the RADIUS servers at *10.6.0.73* and *10.5.0.61* as the second and third RADIUS server to be used for authentication. RADIUS servers are accessed in the order in which they are defined (or for a specified server group, in the order they are defined in the group).
Step 4	**radius-server key** *rad123SN*	Configure the global authentication and encryption key to be used for all RADIUS communications between the SN 5428-2 and the RADIUS daemon. For example, set the key to *rad123SN*. This key must match the key used on the RADIUS daemon.

TACACS+ Hosts

Use the commands in the following procedure to configure TACACS+ authentication services.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**tacacs-server host** *10.7.0.22* **tacacs-server host** *10.7.0.41* **tacacs-server host** *10.7.0.45*	Specify the TACACS+ servers to be used for authentication. For example, specify the TACACS+ servers at *10.7.0.22*, *10.7.0.41*, and *10.7.0.45* for use by the storage router. Because no port is specified, the authentication requests use the default port 49. The global timeout value is also used. Like RADIUS servers, TACACS+ servers are accessed in the order in which they are defined (or for a specified server group, in the order they are defined in the group). See the *Cisco SN 5400 Series Storage Router Command Reference* for more information about the **tacacs-server host** command.
Step 3	**tacacs-server key** *tacacs123SN*	Configure the global authentication and encryption key to be used for all TACACS+ communications between the SN 5428-2 and the TACACS+ servers. For example, set the key to *tacacs123SN*. This key must match the key used by the TACACS+ daemon.

Local Username Database

Use the commands in the following procedure to configure a local username database.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**username** *labserver* **password** *foo* **username** *labserver2* **password** *foo2*	Enter a user name and password for each host requiring authentication prior to access to storage and for each user requiring Monitor mode access to the SN 5428-2 via console, Telnet or SSH management sessions. For example, add the following user name and password combinations: • *labserver* and *foo* • *labserver2* and *foo2* For iSCSI authentication, user name and password pairs must match the CHAP user name and password pairs configured for the iSCSI drivers that require access to storage via the SCSI routing instances that have iSCSI authentication enabled. If other services are also used (such as RADIUS or TACACS+), these user name and password pairs must also be configured within the databases those services use for authentication purposes.

The following rules apply to passwords:

- Passwords are entered in clear text. However, they are changed to "XXXXX" in the CLI command history cache, and are stored in the local username database in an encrypted format.
- If the password contains embedded spaces, enclose it with single or double quotes.
- After initial entry, passwords display in their encrypted format. Use the **show aaa** command to display the local username database entries. The following is an example display:

  ```
  username "foo" password "9 ea9bb0c57ca4806d3555f3f78a4204177a"
  ```

  The initial "9" in the example display indicates that the password is encrypted.
- You can re-enter an encrypted password using the normal **username password** command. Enter the encrypted password in single or double quotes, starting with 9 and a single space. For example, copying and pasting *password "9 ea9bb0c57ca4806d3555f3f78a4204177a"* from the example above into the **username pat** command would create an entry for *pat* in the username database. The user named *pat* would have the same password as the user named *foo*. This functionality allows user names and passwords to be restored from saved configuration files.
- When entering a password, a zero followed by a single space indicates that the following string is not encrypted; 9 followed by a single space indicates that the following string is encrypted. To enter a password that starts with 9 or zero, followed by one or more spaces, enter a zero and a space and then enter the password string. For example, to enter the password "*0 123*" for the user named *pat*, enter this command:

  ```
  username pat password "0 0 123"
  ```

  To enter the password "*9 73Zjm 5*" for user name *lab1*, use this command:

  ```
  username lab1 password '0 9 73Zjm 5'
  ```

Enable

Enable is a special authentication service; it is available for Enable and Login authentication only. The Enable service compares the password you entered with the Administrator mode password configured for the storage router. The requested access is granted only if the passwords match.

See Chapter 3, "Configuring System Parameters," for more information about changing the Administrator mode password.

Monitor

Monitor is a special authentication service; it is available for Enable and Login authentication only. The Monitor service compares the password you entered with the Monitor mode password configured for the storage router. The requested access is granted only if the passwords match.

See Chapter 3, "Configuring System Parameters," for more information about changing the Monitor mode password.

Creating Named Server Groups

By default, you can use all configured RADIUS or TACACS+ servers for authentication. All configured RADIUS servers belong to the default group named *radius. A*ll configured TACACS+ servers belong to the default group named *tacacs+*.

You can also create named groups of RADIUS or TACACS+ servers, to be used for specific authentication purposes. For example, you can use a subset of all configured RADIUS servers for iSCSI authentication of IP hosts requesting access to storage via a specific SCSI routing instance.

In the example configuration shown in Figure 9-2, the group of RADIUS servers named *janus* and the default group of all TACACS+ servers will be used for iSCSI authentication of IP hosts accessing storage via the SCSI routing instance named *zeus*. In the example configurations shown in Figure 9-5 and Figure 9-7, the group of TACACS+ servers named *sysadmin* will be used for Enable and Login authentication.

Radius Server Groups

Use the commands in the following procedure to create a named group of RADIUS servers.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa group server radius** *janus*	Create a group of RADIUS servers. For example create a group named *janus*. All authentication server groups must have unique names; you cannot have a group of RADIUS servers named *janus* and a group of TACACS+ servers named *janus*.
Step 3	**aaa group server radius janus server** *10.5.0.61*	Add a RADIUS server to the named group. For example, add the RADIUS server at IP address *10.5.0.61* to the group named *janus*. Because no port is specified, authentication requests to this server use the default UDP port 1645. Servers are accessed in the order in which they are defined within the named group.
Step 4	**aaa group server radius janus server** *10.6.0.53*	Add another RADIUS server to the named group. For example, add the RADIUS server at IP address *10.6.0.53* to the group named *janus*.

TACACS+ Server Groups

Use the commands in the following procedure to create a named group of TACACS+ servers.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa group server tacacs+** *sysadmin*	Create a group of TACACS+ servers. For example create a group named *sysadmin*. All authentication server groups must have unique names; you cannot have a group of TACACS+ servers named *sysadmin* and a group of RADIUS servers named *sysadmin*.

	Command	Description
Step 3	**aaa group server tacacs+ sysadmin server** *10.7.0.22*	Add a TACACS+ server to the named group. For example, add the TACACS+ server at IP address *10.7.0.22* to the group named *sysadmin*. Because no port is specified, authentication requests to this server use the default port 49. Servers are accessed in the order in which they are defined within the named group.
Step 4	**aaa group server tacacs+ sysadmin server** *10.7.0.41*	Add another TACACS+ server to the named group. For example, add the TACACS+ server at IP address *10.7.0.41* to the group named *sysadmin*.

Creating Authentication Lists

iSCSI, Enable and Login authentication use lists of defined authentication services to administer security functions. The list that is created for Enable and Login authentication must be named *default*. iSCSI authentication supports a variety of authentication lists.

Use the procedures that follow according to the type of authentication required:

- iSCSI authentication
- Enable authentication
- Login authentication

iSCSI authentication

Use the commands in the following procedure to build a unique list of authentication services to be used for iSCSI authentication.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa authentication iscsi** *webservices2* **local group** *janus* **group tacacs+**	Create a unique list of authentication services for iSCSI authentication. For example, create the list called *webservices2* so that AAA first tries to perform authentication using the local username database. If AAA fails to find a user name match, an attempt is made to contact a RADIUS server in the server group named *janus*. If no RADIUS server in group janus is found, RADIUS returns an error and AAA tries to use perform authentication using all configured TACACS+ servers. If no TACACS+ server is found, TACACS+ returns an error and authentication fails. If a RADIUS or TACACS+ server does not find a user name and password match, authentication fails and no other methods are attempted.

Note If local or local-case is the first service in the authentication list and a user name match is not found, the next service in the list will be tried. If local or local-case is not the first service, authentication fails if a user name match is not found. Authentication always fails if a RADIUS or TACACS+ server fails to find a user name match.

Enable authentication

Use the commands in the following procedure to build a default list of authentication services to be used for Enable authentication. Building the default list completes the configuration of Enable authentication and makes it immediately effective.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa authentication enable default group** *sysadmin* **enable**	Create a default list of authentication services for Enable authentication. For example, create a list so that AAA first tries to perform authentication using the TACACS+ servers in the group named *sysadmin*. If no TACACS+ server is found, TACACS+ returns an error and AAA attempts authentication using the configured Administrator mode password. If the password you entered does not match the configured Administrator mode password, authentication fails and no other methods are attempted.

- RADIUS servers are passed the default user name, *$enab15$,* along with the entered password for authentication purposes.
- TACACS+ servers are passed the user name used at login, along with the entered password, for authentication purposes. If a user name was not needed for login, the storage router prompts the user to enter a user name, along with the enable password, when the **enable** command is issued.

Tip You must configure the databases used by the RADIUS or TACACS+ servers with the appropriate user name and password information.

Note Local and local-case services cannot be used for Enable authentication.

Login authentication

Use the commands in the following procedure to build a default list of authentication services to be used for Login authentication. Building the default list completes the configuration of Login authentication and makes it immediately effective.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa authentication login default group** *sysadmin* **monitor**	Create a default list of authentication services for Login authentication. For example, create a list so that AAA first tries to perform authentication using the TACACS+ servers in the group named *sysadmin*. If no TACACS+ server is found, TACACS+ returns an error and AAA attempts authentication using the configured Monitor mode password (eliminating authentication of the user name). If the password you entered does not match the configured Monitor mode password, authentication fails and no other methods are attempted.

Testing Authentication

You can perform authentication testing at any time. For example, before enabling iSCSI authentication for a SCSI routing instance, you can test iSCSI authentication. The user name and password are passed to AAA, which performs authentication using the specified iSCSI authentication list.

The command response indicates a pass or fail status.

iSCSI Authentication

Use the commands in the following procedure to test iSCSI authentication.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa test authentication iscsi** *webservices2 labserver foo* **aaa test authentication iscsi** *webservices2 labserver2 foo2*	Test the user names and passwords listed in the username database. AAA uses the services in the authentication list named *webservices2* for authentication (Example 9-1).

Example 9-1 Testing iSCSI Authentication

```
*[SN5428-2-MG1]# aaa test authentication iscsi webservices2 labserver foo
Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass
```

Enable Authentication

Use the commands in the following procedure to test Enable authentication.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa test authentication enable default** *$enab15$ ciscoadmin*	Test the password configured for Administrator mode access to the storage router, using the default user name passed to RADIUS servers. AAA uses the services in the default authentication list (Example 9-2).

Example 9-2 Testing Enable Authentication

```
*[SN5428-2-MG1]# aaa test authentication enable default $enab15$ ciscoadmin
Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass
```

Login Authentication

Use the commands in the following procedure to test Login authentication.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**aaa test authentication login default** *sysmonitor ciscomonitor*	Test the user name and password configured for Monitor mode access to the storage router. AAA uses the services in the default authentication list (Example 9-3).

Example 9-3 Testing Login Authentication

```
*[SN5428-2-MG1]# aaa test authentication login default sysmonitor ciscomonitor
Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request being queued

Sep 02 14:37:00:aaa:AS_NOTICE :Auth test request complete, status = pass
```

Configuring Two-Way Authentication

When iSCSI authentication is enabled, the SCSI routing instance must authenticate the IP host during the iSCSI TCP connection process. IP hosts that cannot be authenticated are not allowed access to the storage resources. IP hosts may also require authentication of the SCSI routing instance during the iSCSI TCP connection process. If the SCSI routing instance cannot be authenticated, the IP host terminates the connection.

Use the commands in the following procedure to configure a user name and password for a SCSI routing instance that must be authenticated by IP hosts.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**scsirouter** *zeus* **username** *zeusabc*	Assign a user name to the SCSI routing instance. For example, configure the user name *zeusabc* for the SCSI routing instance named *zeus*.
Step 3	**scsirouter** *zeus* **password** *zeus123*	Assign a password to the SCSI routing instance. For example, configure the password *zeus123* for the SCSI routing instance named *zeus*.

Note The SCSI routing instance user name and password pair must also be configured within the authentication database services used by the IP hosts for authentication purposes.

Enabling iSCSI Authentication

iSCSI authentication is enabled for specific SCSI routing instances. By default, iSCSI authentication is not enabled.

Use the commands in the following procedure to enable iSCSI authentication using the authentication services configured in the specified authentication list.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**scsirouter** *zeus* **authentication** *webservices2*	Enable authentication for the named SCSI routing instance, using the named authentication list. For example, enable authentication for the SCSI routing instances named *zeus*, using the authentication list named *webservices2*.

Verifying and Saving Configuration

You can save the configuration at any time using either the **save aaa bootconfig** or **save all bootconfig** commands. Although AAA configuration changes are effective immediately, you must save the authentication configuration for it to be retained in the SN 5428-2 when it is rebooted.

Use the following procedure to verify and save authentication settings.

	Command	Description
Step 1	**enable**	Enter Administrator mode.
Step 2	**show aaa**	Display AAA configuration (Example 9-4).
Step 3	**show scsirouter** *zeus* **brief**	Verify that iSCSI authentication is enabled and (optionally) that the appropriate user name and password are configured for the specified SCSI routing instance. For example, verify that the SCSI routing instance named *zeus* is enabled for authentication using the authentication list named *webservices2* and is configured with the user name *zeusabc* and password *zeus123* (Example 9-5).
Step 4	**save aaa bootconfig**	Save authentication settings.
Step 5	**save scsirouter** *zeus* **bootconfig**	Save the SCSI routing instances.
Step 6	**save all bootconfig**	(Optional) Save all configuration settings. This command may be used in place of individual **save aaa bootconfig** and **save scsirouter bootconfig** commands described in Steps 4 and 5.

Example 9-4 Display AAA Configuration

```
[SN5428-2-MG1]# show aaa
aaa new-model
username "labserver" password "9 491c083a73d7f89bc0205927d086cdd0d8"
username "labserver2" password "9 5ccd52d543e0d3a5558afe8cbe2867dd41"
radius-server key "9 64ced29a261a8ca554a6f4ea8d494669c1"
radius-server host 10.6.0.53 auth-port 1645
radius-server host 10.6.0.73 auth-port 1645
radius-server host 10.5.0.61 auth-port 1645
tacacs-server key "9 c5fc960c37b1a3ad4d76e2495b169e4b08"
tacacs-server host 10.7.0.22 auth-port 49
tacacs-server host 10.7.0.41 auth-port 49
tacacs-server host 10.7.0.45 auth-port 49
aaa group server radius "janus"
aaa group server radius "janus" server 10.5.0.61 auth-port 1645
aaa group server radius "janus" server 10.6.0.53 auth-port 1645
aaa group server tacacs+ "sysadmin"
aaa group server tacacs+ "sysadmin" server 10.7.0.22 auth-port 49
aaa group server tacacs+ "sysadmin" server 10.7.0.41 auth-port 49
aaa authentication enable default group sysadmin enable
aaa authentication iscsi webservices2 local group janus group tacacs+
aaa authentication login default group sysadmin monitor
```

Example 9-5 Verify iSCSI Authentication for SCSI Routing Instance

```
[SN5428-2-MG1]# show scsirouter zeus brief
SCSI Router Information
...
SCSI Router Authentication Information
Router               Authentication  Username        Password
-------------------- --------------- --------------- --------
zeus                 webservices2    zeusabc         9 5eaee29546ed37f31d5812ea60eaac1568
...
```